REMARKS

This Application has been carefully reviewed in light of the Advisory Action mailed December 29, 2003. Claims 1, 7, 11, 13, 14, and 20 have been amended. Claim 18 has been canceled. A new Claim 21 has been added. Applicant respectfully requests favorable action in this case.

Amended Claims/New Claim

Amended Claims 1, 7, 13, 14, and 20 are allowable over U.S. Patent 5,319,776 issued to Hile et al. ("*Hile*"). Claim 1 is allowable over *Hile* because *Hile* does not teach or suggest "receiving, at a state machine of an intrusion detection device, an input stream destined for **a first network device to be protected by the intrusion detection device, the input stream received at the state machine prior to reaching the first network device** and comprising a plurality of characters, wherein **the first network device is operable to execute a program**," [emphasis added] as recited by Claim 1. Instead, *Hile* shows a computer system 14 - the intended destination of an input data stream – that is designed to **protect itself** by conducting a virus string search **after** the input data stream is received. For example, *Hile* teaches that CPU 18b and RAM 20 of computer system 14 are designed to perform the virus protection functions that are represented as blocks 30, 32, 34, 36, 38, and 40 in FIGURE 1 of *Hile*. (See column 3, line 61 through column 4, line 26, and FIGURE 1). Thus, *Hile* shows performing the virus detection function **at the intended destination** (computer system 14) of the input data stream, which is different from receiving an input stream at a state machine of an intrusion detection device before the input stream ever reaches its intended destination (a first network device). As such, *Hile* does not show the identified missing limitation of Claim 1.

Examining a potentially virus-infested input stream by an intrusion detection device before the input stream reaches its intended destination computer has several technical advantages. For example, in one embodiment, the probability of infecting a computer with a virus is reduced by performing the intrusion detection service at a separate system that is not part of the protected computer. Any input stream that is detected as an intrusion activity never reaches the protected computer, which eliminates any chance of a virus infection that may be caused by allowing the input stream to enter the protected computer and buffering the input stream at the protected computer. Computer system 14 of *Hile* does not benefit from

this advantage because the input data stream in fact enters and is buffered by computer system 14 (See buffers 30 and 38 of computer system 14, which are described as parts of RAM 20). Another example advantage, in one embodiment of the invention, is that the resources of the protected computer are freed for other computing functions because the protected computer is relieved of the responsibility of protecting itself from an intrusion. Computer system 14, which is the protected computer in *Hile*, does not benefit from this advantage. As shown in FIGURE 1 and described in column 3, line 61 through column 4, line 26 of *Hile*, computer system 14 performs its own intrusion protection using its own CPU 18b and RAM 20, which indicates that all of the resources for performing intrusion protection is being provided by computer system 14.

It has been suggested in previous Official Actions that destination storage medium 24b of *Hile* constitutes "a first network device" of Claim 1. Such a suggestion was incorrect but clearly does not apply to the amended Claim 1. As recited by Claim 1, " . . . the first network device is operable to execute a program and make a decision according to the program based on data stored in a storage medium of the first network device." In light of this limitation, storage medium 24b cannot be said to constitute first network device of Claim 1 because destination storage medium 24b is not described as a device operable to execute a program and make a decision according to the program. Because *Hile* does not teach or suggest the identified missing limitations, Claim 1 is allowable. Favorable action is requested.

Claims 7, 13, 14, and 20 are allowable for reasons analogous to those provided in conjunction with Claim 1. Favorable action is requested.

As depending from their respectively allowable independent Claims 1, 7, 13, 14, and 20, dependent Claims 2-6, 8-12, 15-19, and 21 are also allowable. Claim 21 is also allowable because *Hile* does not teach or suggest "wherein the first character and the next character are each selected and compared **only once**," [emphasis added] as recited by Claim 21. In some embodiments, this is advantageous because such an intrusion protection procedure consumes less resources of the intrusion detection device. While *Hile* appears to show examining the characters of an input data stream, *Hile* does not show examining each character "only once." As such, Claim 20 is allowable. Favorable action is requested.

Conclusions

Applicants have made an earnest attempt to place this case in condition for allowance. For the foregoing reasons, and for other reasons clearly apparent, Applicants respectfully request full allowance of all pending Claims.

If the Examiner feels that a telephone conference or an interview would advance prosecution of this Application in any manner, the undersigned attorney for Applicants stands ready to conduct such a conference at the convenience of the Examiner.

A check for $750.00 is enclosed to cover the fee for the RCE. However, the Commissioner is hereby authorized to charge any required fee to Deposit Account No. 02-0384 of Baker Botts, LLP.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicant

Bradley P. Williams
Reg. No. 40,227

Date: March 29, 2004

Correspondence Address:
2001 Ross Avenue, Suite 600
Dallas, Texas 75201-2980
Phone: (214) 953-6447

Customer Number: **05073**